Podręcznik zarządzania komputerami typu Desktop

Komputery Business Desktop

Numer katalogowy dokumentu: 312947-242

Wrzesień 2003

W podręczniku tym zawarte są definicje i instrukcje dotyczące korzystania z funkcji zabezpieczeń oraz systemu inteligentnego zarządzania Intelligent Manageability, które są zainstalowane fabrycznie na wybranych modelach stacji roboczych i komputerów typu Desktop

OSTRZEŻENIE: Tak oznaczane są zalecenia, których nieprzestrzeganie może doprowadzić do obrażeń ciała lub śmierci.

PRZESTROGA: Tak oznaczane są zalecenia, których nieprzestrzeganie może doprowadzić do uszkodzenia sprzętu lub utraty danych.

Podręcznik zarządzania komputerami typu Desktop
Komputery Business Desktop

Wydanie drugie — Wrzesień 2003
Numer katalogowy dokumentu: 312947-242

Spis treści

Podręcznik zarządzania komputerami typu Desktop

Indeks

Podręcznik zarządzania komputerami typu Desktop

Stworzony przez firmę HP system Intelligent Manageability obejmuje standardowe rozwiązania służące do sterowania i sprawowania nadzoru nad komputerami stacjonarnymi, przenośnymi i stacjami roboczymi w środowisku sieciowym. W 1995 roku firma HP — jako pierwsza w branży — wprowadziła na rynek rodzinę komputerów osobistych typu Desktop z zaimplementowaną funkcją zdalnego zarządzania. Firma HP posiada patent na technologię zarządzania. Od tego czasu prowadzone były — zakrojone na szeroką skalę — prace mające na celu rozwój standardów i infrastruktury, pozwalających na efektywne rozmieszczanie i konfigurowanie komputerów stacjonarnych, przenośnych i stacji roboczych oraz zarządzanie nimi. W związku z tym podjęto ścisłą współpracę z wiodącymi producentami oprogramowania, co umożliwiło zachowanie zgodności między dostarczanymi przez nich programami a systemem Intelligent Manageability. System ten jest istotnym elementem prowadzonych działań, których celem jest opracowanie rozwiązań wspomagających decyzje klientów podczas czterech faz cyklu życia komputerów typu Desktop — planowania, rozmieszczania, zarządzania i unowocześniania.

Najważniejsze funkcje i możliwości zarządzania komputerami typu Desktop to:

- Początkowa konfiguracja i rozmieszczanie
- Zdalne instalowanie systemu
- Aktualizowanie programów i zarządzanie nimi
- Pamięć ROM typu flash
- Śledzenie i funkcje zabezpieczeń zasobów
- Powiadamianie o usterkach i ich usuwanie

Obsługa poszczególnych funkcji opisanych w tym dokumencie może się różnić w zależności od modelu lub wersji oprogramowania.

Początkowa konfiguracja i rozmieszczanie

Komputer został dostarczony wraz z preinstalowanym obrazem oprogramowania systemowego. Dzięki temu po szybkim „rozpakowaniu" oprogramowania komputer jest gotowy do pracy.

Użytkownik może zastąpić preinstalowany obraz oprogramowania dowolnym systemem operacyjnym i aplikacjami dostosowanymi do własnych potrzeb. Istnieje kilka metod rozmieszczania takiego oprogramowania. Zostały one wymienione poniżej:

- Zainstalowanie dodatkowych aplikacji po rozpakowaniu preinstalowanego obrazu oprogramowania.
- Zastąpienie preinstalowanego oprogramowania dostosowanym obrazem oprogramowania za pomocą narzędzi rozmieszczania (np. Altiris Deployment Solution™).
- Skopiowanie zawartości jednego dysku twardego na inny (w ramach procesu klonowania danych).

Najlepsza metoda rozmieszczania zależy od charakteru środowiska informatycznego oraz realizowanych w nim procesów. Informacje pomocne w wyborze tej metody można uzyskać w części dotyczącej rozmieszczania komputera, dostępnej w witrynie sieci Web poświęconej zalecanym rozwiązaniom i oferowanym usługom (http://h18000.www1.hp.com/solutions/pcsolutions).

Informacje o odzyskiwaniu oprogramowania systemowego, zarządzaniu konfiguracją i energią oraz rozwiązywaniu problemów można znaleźć na dysku CD *Restore Plus!*, a także w dokumentacji dotyczącej programu Computer Setup i sprzętu obsługującego funkcję ACPI.

Zdalne instalowanie systemu

Funkcja zdalnego instalowania systemu umożliwia uruchomienie i skonfigurowanie systemu operacyjnego za pomocą oprogramowania i informacji konfiguracyjnych znajdujących się na serwerze sieciowym, poprzez inicjację środowiska Preboot Execution Environment (PXE). Funkcja zdalnego instalowania systemu służy zazwyczaj do instalowania i konfigurowania systemu operacyjnego, lecz może również zostać użyta do przeprowadzenia następujących zadań:

- formatowanie dysku twardego,
- rozmieszczanie obrazu oprogramowania na jednym lub kilku nowych komputerach,
- zdalne aktualizowanie systemu BIOS w pamięci ROM typu flash („Zdalne zarządzanie pamięcią ROM typu flash" na stronie 8),
- konfigurowanie ustawień systemu BIOS.

Aby rozpocząć proces zdalnego instalowania systemu, należy nacisnąć klawisz **F12** (po pojawieniu się — w prawym dolnym rogu ekranu z logo firmy HP — komunikatu „F12 = Network Service Boot"), a następnie postępować zgodnie z wyświetlanymi instrukcjami. Domyślna kolejność uruchamiania jest ustawieniem konfiguracyjnym systemu BIOS, które można zmienić na opcję podejmowania każdorazowo próby uruchomienia środowiska PXE.

Firmy HP oraz Altiris wspólnie opracowały narzędzia pozwalające na łatwiejsze i szybsze przeprowadzanie rozmieszczania komputerów oraz zarządzanie nimi w ramach przedsiębiorstwa. Dzięki znacznemu obniżeniu całkowitych kosztów związanych z wdrożeniem systemu informatycznego, komputery klienckie firmy HP stanowią najodpowiedniejsze — pod kątem zarządzania — rozwiązanie dla przedsiębiorstwa.

Aktualizowanie oprogramowania i zarządzanie nim

Firma HP udostępnia kilka narzędzi służących do zarządzania oprogramowaniem zainstalowanym na komputerach typu Desktop i stacjach roboczych oraz aktualizowania go — Altiris, Altiris PC Transplant Pro, HP Client Manager Software, Altiris Solution, System Software Manager, Proactive Change Notification oraz ActiveUpdate.

HP Client Manager Software

Oprogramowanie HP Client Manager Software (HP CMS) ściśle integruje technologię HP Intelligent Manageability w ramach narzędzia Altiris, zapewniając niezrównane możliwości zarządzania sprzętem dla urządzeń dostępowych firmy HP, takie jak:

- Szczegółowe widoki spisu sprzętu dla celów zarządzania zasobami.
- Monitorowanie stanu komputera i diagnostyka.
- Proaktywne powiadomienia o zmianach w środowisku sprzętowym.
- Dostępne poprzez sieć Web raporty o szczegółach krytycznych dla działalności, takich jak komputery z ostrzeżeniami termicznymi, alerty pamięci i wiele innych.
- Zdalne aktualizowanie oprogramowania systemowego, np. sterowników sprzętowych i pamięci ROM BIOS.
- Zdalna zmiana kolejności uruchamiania.

Więcej informacji o oprogramowaniu HP Client Manager można znaleźć na stronie: http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Solutions

Oprogramowanie HP Client Manager Solutions zapewnia scentralizowane zarządzanie sprzętem urządzeń klienckich firmy HP dla wszystkich obszarów cyklów życia IT.

- Zarządzanie spisem i zasobami
  - Zgodność licencji na oprogramowanie
  - Śledzenie komputera i generowanie raportów
  - Śledzenie kontraktów leasingowych i środków trwałych
- Rozmieszczanie i migracja
  - Migracja systemu Microsoft Windows 2000 lub Windows XP Professional bądź Home Edition
  - Rozmieszczanie systemu
  - Migracje osobowości
- Punkt pomocy i rozwiązywanie problemów
  - Zarządzanie kuponami punktu pomocy
  - Zdalne usuwanie problemów
  - Zdalne rozwiązywanie problemów
  - Odzyskiwanie komputerów klienckich po awarii
- Zarządzanie oprogramowaniem i operacjami
  - Bieżące zarządzanie komputerami typu Desktop
  - Rozmieszczanie oprogramowania systemowego firmy HP
  - Samonaprawianie aplikacji

W przypadku wybranych modeli komputerów stacjonarnych i przenośnych w skład fabrycznie załadowanego obrazu wchodzi agent zarządzania Altiris. Agent ten umożliwia komunikację z oprogramowaniem Altiris Development Solution, za pomocą którego można wykonać nowe rozmieszczanie sprzętu lub migrację osobowości do nowego systemu operacyjnego przy użyciu prostych w obsłudze kreatorów. Rozwiązanie Altiris stanowi wygodne narzędzie dystrybucji oprogramowania. Używane w połączeniu z oprogramowaniem System Software Manager lub HP Client Manager, umożliwia też administratorom aktualizowanie oprogramowania ROM BIOS oraz sterowników urządzeń z poziomu centralnej konsoli.

Więcej informacji można znaleźć na stronie http://www.hp.com/go/easydeploy.

Altiris PC Transplant Pro

Narzędzie Altiris PC Transplant Pro umożliwia bezproblemową migrację komputera, zachowując stare ustawienia, preferencje i dane oraz migrując je do nowego środowiska w szybki i prosty sposób. Czas trwania uaktualnień jest liczony w minutach, a nie w godzinach czy dniach, natomiast pulpit wygląda i działa dokładnie tak, jak tego oczekuje użytkownik.

Więcej informacji oraz szczegóły dotyczące pobierania w pełni funkcjonalnej 30-dniowej wersji ewaluacyjnej można znaleźć na stronie http://h18000.www1.hp.com/im/prodinfo.html#deploy.

System Software Manager

Program narzędziowy System Software Manager (SSM) służy do równoczesnego aktualizowania oprogramowania systemowego zainstalowanego w różnych systemach. Po jego uruchomieniu na komputerze klienckim wykrywane są wersje sprzętu i oprogramowania, a następnie wybrane programy są aktualizowane plikami pochodzącymi z repozytorium centralnego, zwanego także magazynem plików. Wersje sterowników obsługiwane przez oprogramowanie SSM są oznaczone specjalną ikoną w witrynie pobierania sterowników oraz na dysku CD Support Software. Aby pobrać oprogramowanie SSM i uzyskać więcej informacji na jego temat, należy odwiedzić stronę: http://h18000.www1.hp.com/im/ssmwp.html.

Proactive Change Notification

Program Proactive Change Notification używa bezpiecznej witryny internetowej w celu proaktywnego i automatycznego wykonywania następujących zadań:

- Wysyłanie pocztą e-mail proaktywnych powiadomień o zmianach (Proactive Change Notification — PCN), które z nawet 60-dniowym wyprzedzeniem informują o zmianach w sprzęcie i oprogramowaniu dla większości komercyjnych komputerów i serwerów.
- Wysyłanie wiadomości e-mail zawierających biuletyny, porady dla klientów, ważne informacje, biuletyny dotyczące zabezpieczeń oraz alerty sterowników dla większości komercyjnych komputerów i serwerów.

Użytkownik tworzy swój własny profil w celu zapewnienia sobie otrzymywania tylko informacji związanych z określonym środowiskiem informatycznym. Aby uzyskać więcej informacji o programie Proactive Change Notification i utworzyć profil niestandardowy, należy odwiedzić stronę http://www.hp.com/go/pcn.

ActiveUpdate

ActiveUpdate to aplikacja kliencka firmy HP. Klient ActiveUpdate jest uruchamiany w systemie lokalnym i, korzystając ze zdefiniowanego przez użytkownika profilu, proaktywnie i automatycznie pobiera aktualizacje oprogramowania dla większości komercyjnych komputerów i serwerów firmy HP. Pobrane aktualizacje mogą zostać automatycznie rozmieszczone na komputerach, dla których są przeznaczone w ramach oprogramowania HP Client Manager Software oraz System Software Manager.

Aby uzyskać więcej informacji o rozwiązaniu ActiveUpdate, pobrać aplikację i utworzyć profil niestandardowy, należy odwiedzić stronę: http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html.

Pamięć ROM typu flash

Komputer jest standardowo wyposażony w programowalną pamięć ROM (read only memory) typu flash. W celu zabezpieczenia jej przed nieumyślnym zaktualizowaniem lub zastąpieniem można ustawić hasło konfiguracyjne w programie Computer Setup (F10). Zapewni to operacyjną integralność komputera. Jeżeli zajdzie potrzeba uaktualnienia pamięci ROM, można:

- zamówić u przedstawiciela firmy HP dyskietkę zawierającą uaktualniony pakiet ROMPaq,
- pobrać najnowsze pliki ROMPaq z witryny http://h18000.www1.hp.com/im/ssmwp.html.

PRZESTROGA: Aby zapewnić maksymalną ochronę pamięci ROM, trzeba pamiętać o ustawieniu hasła konfiguracyjnego. Hasło konfiguracyjne zapobiega nieautoryzowanym uaktualnieniom pamięci ROM. Za pomocą programu System Software Manager administrator systemu może jednocześnie ustawić takie hasło na jednym lub kilku komputerach pracujących w sieci. Więcej informacji można znaleźć w witrynie: http://h18000.www1.hp.com/im/ssmwp.html.

Zdalne zarządzanie pamięcią ROM typu flash

Funkcja zdalnego zarządzania pamięcią ROM typu flash umożliwia administratorowi systemu zdalne uaktualnianie pamięci ROM komputerów HP pracujących w sieci z jednej centralnej konsoli administracyjnej. Dzięki niej wprowadzane zmiany są identyczne na wszystkich komputerach, a administrator ma większą kontrolę nad procesem uaktualniania zawartości pamięci ROM na sieciowych komputerach firmy HP. W rezultacie ulega poprawie wydajność pracy oraz obniżają się ogólne koszty związane z eksploatacją sieci w przedsiębiorstwie.

Aby możliwe było skorzystanie z funkcji zdalnego zarządzania pamięcią ROM typu flash, komputer musi zostać włączony ręcznie lub zdalnie za pomocą funkcji zdalnego przywracania ze stanu wstrzymania (Remote Wakeup).

Więcej informacji o zdalnym zarządzaniu pamięcią ROM typu flash można znaleźć w części poświęconej programowi HP Client Manager Software lub System Software Manager na stronie http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

Program narzędziowy HPQFlash służy do lokalnego aktualizowania lub przywracania systemowej pamięci ROM na pojedynczych komputerach poprzez system operacyjny Windows.

Więcej informacji o programie HPQFlash można znaleźć na stronie http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html.

Bezpieczny blok uruchamiania pamięci ROM

Bezpieczny blok uruchamiania pamięci ROM (FailSafe Boot Block ROM) umożliwia odzyskiwanie zasobów systemowych w przypadku nieudanej aktualizacji pamięci ROM typu flash (np. w razie awarii zasilania podczas aktualizacji tej pamięci). Blok ten stanowi część pamięci ROM, jest jednak zabezpieczony przed aktualizacją. Jego zadaniem jest sprawdzanie poprawności zawartości pamięci ROM typu flash po włączeniu zasilania systemu.

- Jeżeli sprawdzenie poprawności przebiegnie pomyślnie, system zostanie uruchomiony w zwykły sposób.
- Jeżeli w systemowej pamięci ROM zostaną wykryte błędy, bezpieczny blok uruchamiania umożliwi uruchomienie systemu z dyskietki ROMPaq, która przeprogramuje uszkodzoną pamięć.

Jeżeli blok uruchamiania wykryje nieprawidłową systemową pamięć ROM, dioda zasilania zamiga osiem razy (kolor czerwony) w odstępach jednosekundowych, po czym nastąpi 2-sekundowa pauza. Odtworzonych też zostanie 8 sygnałów dźwiękowych. Na ekranie zostanie wyświetlony komunikat o pracy w trybie odzyskiwania bloku uruchamiania (niektóre modele).

Aby odzyskać system po uruchomieniu go w trybie odzyskiwania bloku uruchamiania:

1. Jeżeli w napędzie dyskietek znajduje się dyskietka, wyjmij ją, a następnie wyłącz zasilanie.
2. Włóż dyskietkę ROMPaq do napędu dyskietek.
3. Włącz zasilanie systemu.
4. Jeżeli dyskietka ROMPaq nie zostanie znaleziona, pojawi się monit o jej włożenie do napędu i ponowne uruchomienie komputera.

5. Jeżeli ustawiono hasło konfiguracyjne, włączy się wskaźnik Caps Lock na klawiaturze i pojawi się monit o wprowadzenie hasła.
6. Wprowadź hasło konfiguracyjne.
7. Włączenie się wszystkich trzech diod klawiatury po uruchomieniu systemu z dyskietki oznacza, że pamięć ROM została pomyślnie przeprogramowana. Gdy proces dobiegnie końca, zostanie również wyemitowana seria sygnałów dźwiękowych o coraz wyższej częstotliwości.
8. Wyjmij dyskietkę i wyłącz zasilanie.
9. Włącz zasilanie, aby uruchomić ponownie komputer.

Poniższa tabela zawiera wykaz kombinacji wskaźników klawiatury używanych przez blok uruchamiania pamięci ROM (gdy do komputera jest podłączona klawiatura PS/2), jak również znaczenie i stan związany z każdą kombinacją.

Kombinacje wskaźników klawiatury używane przez blok uruchamiania pamięci ROM

Tryb bezpiecznego bloku uruchamiania	Kolor diody na klawiaturze	Stan diody na klawiaturze	Stan/Komunikat
Num Lock	Zielony	Włączona	Brak dyskietki ROMPaq, dyskietka jest uszkodzona lub napęd nie jest gotowy.
Caps Lock	Zielony	Włączona	Wprowadź hasło.
Num, Caps, Scroll Lock	Zielony	Migają pojedynczo w następującej kolejności: Num, Caps, Scroll Lock	Klawiatura jest zablokowana w trybie sieciowym.
Num, Caps, Scroll Lock	Zielony	Włączona	Blok uruchamiania pamięci ROM typu flash — operacja zakończona pomyślnie. Wyłącz zasilanie, a następnie uruchom komputer ponownie.

Wskaźniki diagnostyczne nie migają w przypadku klawiatury podłączonej przez złącze USB.

Replikowanie ustawień konfiguracyjnych

Przy użyciu poniższych procedur administrator może w prosty sposób kopiować ustawienia konfiguracyjne z jednego komputera na inne (ten sam model). Umożliwia to zachowanie zgodności danych konfiguracyjnych na wielu komputerach.

W przypadku obu procedur wymagany jest napęd dyskietek lub obsługiwane urządzenie USB typu flash, np. HP Drive Key.

Kopiowanie na jeden komputer

PRZESTROGA: Ustawienia konfiguracyjne są specyficzne dla modelu komputera. Jeśli modele komputera źródłowego i docelowego są różne, może dojść do uszkodzenia systemu plików. Przykładowo nie należy kopiować ustawień konfiguracyjnych z komputera D510 w ultracienkiej obudowie typu Desktop do komputera D510 e-pc.

1. Wybierz ustawienia konfiguracyjne do skopiowania. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

3. Włóż dyskietkę lub urządzenie USB typu flash.
4. Kliknij kolejno **File (Plik) > Save to Diskette (Zapisz na dyskietce)**. Postępuj zgodnie z instrukcjami pojawiającymi się na ekranie, aby zapisać ustawienia konfiguracyjne na dyskietce lub w urządzeniu USB typu flash.
5. Wyłącz komputer, który ma zostać skonfigurowany, a następnie włóż dyskietkę konfiguracyjną do napędu lub podłącz urządzenie USB typu flash.

6. Włącz komputer. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.
7. Kliknij kolejno **File (Plik) > Restore from Diskette (Odtwórz z dyskietki)**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
8. Po ukończeniu konfiguracji uruchom ponownie komputer.

Kopiowanie na wiele komputerów

PRZESTROGA: Ustawienia konfiguracyjne są specyficzne dla modelu komputera. Jeśli modele komputera źródłowego i docelowego są różne, może dojść do uszkodzenia systemu plików. Przykładowo nie należy kopiować ustawień konfiguracyjnych z komputera D510 w ultracienkiej obudowie typu Desktop do komputera D510 e-pc.

Wprawdzie przygotowanie dyskietki konfiguracyjnej lub urządzenia USB typu flash przy użyciu tej metody trwa nieznacznie dłużej, ale dane są kopiowane na komputery docelowe znacznie szybciej.

Do wykonania tej procedury lub utworzenia rozruchowego urządzenia USB typu flash wymagana jest dyskietka rozruchowa. Dyskietki takiej nie można utworzyć w systemie Windows 2000. Jeśli nie jest dostępny komputer z systemem umożliwiającym utworzenie dyskietki rozruchowej (Windows 9x lub Windows XP), należy skorzystać z metody kopiowania na jeden komputer (zobacz część „Kopiowanie na jeden komputer” na stronie 11).

1. Utwórz dyskietkę rozruchową lub rozruchowe urządzenie USB typu flash. Zobacz część „Dyskietka rozruchowa” na stronie 14, „Obsługiwane urządzenie USB typu flash” na stronie 14 lub „Nieobsługiwane urządzenie USB typu flash” na stronie 18.

PRZESTROGA: Nie wszystkie komputery można uruchomić za pomocą urządzenia USB typu flash. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności uruchamiania urządzeń w programie Computer Setup (F10), taki komputer można uruchomić za pomocą urządzenia USB typu flash. W innym przypadku należy użyć dyskietki rozruchowej.

2. Wybierz ustawienia konfiguracyjne do skopiowania. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
3. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

4. Włóż dyskietkę rozruchową lub rozruchowe urządzenie USB typu flash.
5. Kliknij kolejno **File (Plik) > Save to Diskette (Zapisz na dyskietce)**. Postępuj zgodnie z instrukcjami pojawiającymi się na ekranie, aby zapisać ustawienia konfiguracyjne na dyskietce lub w urządzeniu USB typu flash.
6. Pobierz program narzędziowy BIOS służący do kopiowania ustawień konfiguracyjnych (repset.exe) i skopiuj go na dyskietkę konfiguracyjną lub konfiguracyjne urządzenie USB typu flash. Program ten można znaleźć na stronie http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html.
7. Na dyskietce konfiguracyjnej lub w konfiguracyjnym urządzeniu USB typu flash utwórz plik autoexec.bat zawierający następujące polecenie:

   repset.exe

8. Wyłącz komputer, który ma zostać skonfigurowany. Włóż dyskietkę konfiguracyjną lub konfiguracyjne urządzenie USB typu flash, a następnie włącz komputer. Program konfiguracyjny zostanie uruchomiony automatycznie.
9. Po ukończeniu konfiguracji uruchom ponownie komputer.

Tworzenie urządzenia rozruchowego

Dyskietka rozruchowa

Instrukcje te dotyczą systemów Windows XP Professional i Home Edition. System Windows 2000 nie obsługuje funkcji tworzenia dyskietek rozruchowych.

1. Włóż dyskietkę do napędu dyskietek.
2. Kliknij przycisk **Start**, a następnie polecenie **Mój komputer**.
3. Kliknij prawym przyciskiem myszy napęd dyskietek, a następnie wybierz polecenie **Formatuj**.
4. Zaznacz pole wyboru **Utwórz dysk startowy systemu MS-DOS**, a następnie kliknij przycisk **Rozpocznij**.

Wróć do części „Kopiowanie na wiele komputerów" na stronie 12.

Obsługiwane urządzenie USB typu flash

Obsługiwane urządzenia, takie jak HP Drive Key lub DiskOnKey, są wyposażone w preinstalowany obraz, co upraszcza proces przekształcania ich w urządzenia rozruchowe. Jeśli używane urządzenie Drive Key nie jest wyposażone w taki obraz, należy użyć procedury opisanej dalej w tej części (zobacz „Nieobsługiwane urządzenie USB typu flash" na stronie 18).

PRZESTROGA: Nie wszystkie komputery można uruchomić za pomocą urządzenia USB typu flash. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności uruchamiania urządzeń w programie Computer Setup (F10), taki komputer można uruchomić za pomocą urządzenia USB typu flash. W innym przypadku należy użyć dyskietki rozruchowej.

Aby utworzyć rozruchowe urządzenie USB typu flash, należy korzystać z następujących elementów:

- Jeden z następujących komputerów:
  - Compaq Evo D510 w ultracienkiej obudowie typu Desktop
  - Compaq Evo D510 w przekształcalnej obudowie Minitower/obudowie małowymiarowej
  - HP Compaq Business Desktop, seria d530 — w ultracienkiej obudowie typu Desktop, obudowie małowymiarowej lub przekształcalnej obudowie Minitower
  - Komputery przenośne Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c lub N1000c
  - Komputery przenośne Compaq Presario 1500 lub 2800

  W zależności od indywidualnych ustawień systemu BIOS, przyszłe komputery będą mogły obsługiwać również uruchamianie za pomocą urządzenia HP Drive Key.

PRZESTROGA: Jeśli używany jest komputer inny niż wyżej wymienione, należy upewnić się, czy urządzenie USB jest wymienione przed dyskiem twardym na liście kolejności uruchamiania w programie Computer Setup (F10).

- Jeden z następujących modułów pamięci:
  - HP Drive Key 16 MB
  - HP Drive Key 32 MB
  - DiskOnKey 32 MB
  - HP Drive Key 64 MB
  - DiskOnKey 64 MB
  - HP Drive Key 128 MB
  - DiskOnKey 128 MB
- Dyskietka rozruchowa DOS z programami FDISK i SYS. Jeśli program SYS jest niedostępny, można użyć programu FORMAT, lecz spowoduje to utratę wszystkich plików zapisanych już w urządzeniu Drive Key.

1. Wyłącz komputer.
2. Podłącz urządzenie Drive Key do jednego z portów USB komputera i odłącz wszystkie inne urządzenia pamięci masowej USB (oprócz napędów dyskietek USB).
3. Włóż do napędu dyskietkę rozruchową DOS z programem FDISK.COM oraz programem SYS.COM lub FORMAT.COM. Następnie włącz komputer, aby uruchomić go z dyskietki DOS.
4. Uruchom program FDISK z wiersza A:\, wpisując **FDISK** i naciskając klawisz Enter. Po wyświetleniu monitu kliknij przycisk **Yes** (**Y**), aby włączyć obsługę napędów o dużej pojemności.
5. Wprowadź numer [**5**], aby wyświetlić listę napędów w systemie. Urządzenie Drive Key można zidentyfikować po rozmiarze dysku. Odpowiada mu napęd, którego rozmiar jest najbardziej zbliżony — zazwyczaj ostatni napęd z listy. Zanotuj literę napędu.

   Napęd Drive Key: _____

PRZESTROGA: Jeśli ten napęd nie odpowiada urządzeniu Drive Key, nie należy kontynuować procedury. Może to spowodować utratę danych. Należy sprawdzić wszystkie porty USB pod kątem innych urządzeń pamięci masowej. W przypadku ich znalezienia należy odłączyć te urządzenia, a następnie uruchomić ponownie komputer i kontynuować procedurę od punktu 4. Jeśli takie urządzenia nie zostaną znalezione, może to oznaczać, że system nie obsługuje urządzeń Drive Key lub podłączone urządzenie Drive Key jest uszkodzone. NIE należy kontynuować procedury przekształcania urządzenia Drive Key w urządzenie rozruchowe.

6. Wyjdź z programu FDISK, naciskając klawisz **Esc** w celu powrotu do wiersza A:\.
7. Jeśli dyskietka rozruchowa DOS zawiera program SYS.COM, przejdź do punktu 8. W innym przypadku przejdź do punktu 9.
8. W wierszu A:\ wprowadź polecenie **SYS x:**, gdzie x oznacza zanotowaną wcześniej literę napędu. Przejdź do punktu 13.

PRZESTROGA: Należy pamiętać o wprowadzeniu poprawnej litery napędu dla urządzenia Drive Key.

Po przetransferowaniu plików systemowych program SYS powróci do wiersza A:\.

9. Wybierz pliki, które chcesz zachować, i skopiuj je z urządzenia Drive Key do katalogu tymczasowego na innym dysku (np. wewnętrznym dysku twardym systemu).
10. W wierszu A:\ wprowadź polecenie **FORMAT /S X:**, gdzie X oznacza zanotowaną wcześniej literę napędu.

PRZESTROGA: Należy pamiętać o wprowadzeniu poprawnej litery napędu dla urządzenia Drive Key.

Polecenie FORMAT spowoduje wyświetlenie jednego lub więcej ostrzeżeń i za każdym razem pojawi się pytanie, czy proces ma być kontynuowany. W odpowiedzi należy każdorazowo wpisać literę **y**. Polecenie FORMAT spowoduje sformatowanie urządzenia Drive Key i dodanie plików systemowych. Zostanie również wyświetlone zapytanie o etykietę woluminu.

11. Wprowadź etykietę (jeśli jest potrzebna) lub naciśnij klawisz **Enter**, aby ją pominąć.
12. Skopiuj wszystkie pliki zapisane w punkcie 9 na urządzenie Drive Key.
13. Wyjmij dyskietkę i uruchom ponownie komputer. Komputer zostanie uruchomiony z urządzeniem Drive Key jako dyskiem C.

Na każdym komputerze może być określona inna domyślna kolejność uruchamiania urządzeń — do jej zmiany służy program narzędziowy Computer Setup (F10).

W wersji DOS dla środowiska Windows 9x może się chwilowo pojawić ekran z logo Windows. Jeśli ten ekran nie ma być wyświetlany, w katalogu głównym urządzenia Drive Key należy dodać plik o rozmiarze zerowym i nazwie LOGO.SYS.

Powrót do „Kopiowanie na wiele komputerów” na stronie 12.

Nieobsługiwane urządzenie USB typu flash

PRZESTROGA: Nie wszystkie komputery można uruchomić za pomocą urządzenia USB typu flash. Jeśli urządzenie USB jest wymienione przed dyskiem twardym na liście domyślnej kolejności uruchamiania urządzeń w programie Computer Setup (F10), taki komputer można uruchomić za pomocą urządzenia USB typu flash. W innym przypadku należy użyć dyskietki rozruchowej.

Aby utworzyć rozruchowe urządzenie USB typu flash, należy korzystać z następujących elementów:

- Jeden z następujących komputerów:
  - Compaq Evo D510 w ultracienkiej obudowie typu Desktop
  - Compaq Evo D510 w przekształcalnej obudowie Minitower/obudowie małowymiarowej
  - HP Compaq Business Desktop, seria d530 — w ultracienkiej obudowie typu Desktop, obudowie małowymiarowej lub przekształcalnej obudowie Minitower
  - Komputery przenośne Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c lub N1000c
  - Komputery przenośne Compaq Presario 1500 lub 2800

  W zależności od indywidualnych ustawień systemu BIOS, przyszłe komputery będą mogły obsługiwać również uruchamianie za pomocą urządzenia USB typu flash.

PRZESTROGA: Jeśli używany jest komputer inny niż wyżej wymienione, należy upewnić się, czy urządzenie USB jest wymienione przed dyskiem twardym na liście kolejności uruchamiania w programie Computer Setup (F10).

- Dyskietka rozruchowa DOS z programami FDISK i SYS. Jeśli program SYS jest niedostępny, można użyć programu FORMAT, lecz spowoduje to utratę wszystkich plików zapisanych już w urządzeniu Drive Key.

1. Jeśli w systemie znajdują się karty PCI z dołączonymi napędami SCSI, ATA RAID lub SATA, wyłącz komputer i odłącz kabel zasilający.

PRZESTROGA: Kabel zasilający MUSI być odłączony od gniazda sieci elektrycznej.

2. Zdejmij obudowę komputera i odłącz karty PCI.
3. Podłącz urządzenie USB typu flash do jednego z portów USB komputera i odłącz wszystkie inne urządzenia pamięci masowej USB (oprócz napędów dyskietek USB). Zamknij obudowę komputera.
4. Podłącz kabel zasilający i włącz komputer. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**, aby przejść do programu konfiguracyjnego komputera.
5. Wybierz menu Advanced (Zaawansowane), opcję PCI devices (Urządzenia PCI), aby wyłączyć kontrolery IDE i SATA. Wyłączając kontroler SATA należy zanotować przerwanie IRQ, do którego jest on przypisany. Informacja ta będzie później potrzebna do ponownego przypisania przerwania IRQ. Zamknij program konfiguracyjny i potwierdź zmiany.

   Przerwanie IRQ SATA: _____
6. Włóż do napędu dyskietkę rozruchową DOS z programem FDISK.COM oraz programem SYS.COM lub FORMAT.COM. Następnie włącz komputer, aby uruchomić go z dyskietki DOS.
7. Uruchom program FDISK i usuń wszystkie istniejące partycje urządzenia USB typu flash. Utwórz nową partycję i oznacz ją jako aktywną. Zamknij program FDISK, naciskając klawisz **Esc**.
8. Jeśli po zamknięciu programu FDISK system nie zostanie automatycznie ponownie uruchomiony, naciśnij kombinację klawiszy **Ctrl**+**Alt**+**Del**, aby ponownie uruchomić system z dyskietki DOS.
9. W wierszu A:\ wprowadź polecenie **FORMAT C: /S** i naciśnij klawisz **Enter**. Spowoduje to sformatowanie urządzenia USB typu flash i dodanie plików systemowych. Zostanie również wyświetlone zapytanie o etykietę woluminu.
10. Wprowadź etykietę (jeśli jest potrzebna) lub naciśnij klawisz **Enter**, aby ją pominąć.

11. Wyłącz komputer i odłącz kabel zasilający. Otwórz obudowę komputera i ponownie zainstaluj wszystkie odłączone wcześniej karty PCI. Zamknij obudowę komputera.
12. Podłącz kabel zasilający, wyjmij z napędu dyskietkę, a następnie włącz komputer.
13. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**, aby przejść do programu konfiguracyjnego komputera.
14. Wybierz menu Advanced (Zaawansowane), opcję PCI devices (Urządzenia PCI) i ponownie włącz kontrolery IDE i SATA, które zostały wyłączone w punkcie 5. Przypisz kontroler SATA do jego pierwotnego przerwania IRQ.
15. Zapisz zmiany i zakończ pracę programu. Komputer zostanie uruchomiony z urządzeniem USB typu flash jako dyskiem C.

Na każdym komputerze może być określona inna domyślna kolejność uruchamiania urządzeń — do jej zmiany służy program narzędziowy Computer Setup (F10).

W wersji DOS dla środowiska Windows 9x może się chwilowo pojawić ekran z logo Windows. Jeśli ten ekran nie ma być wyświetlany, w katalogu głównym urządzenia Drive Key należy dodać plik o rozmiarze zerowym i nazwie LOGO.SYS.

Powrót do „Kopiowanie na wiele komputerów” na stronie 12.

Dwufunkcyjny przycisk zasilania

W systemach Windows 2000 oraz Windows XP Professional i Home Edition z aktywnym interfejsem zaawansowanego zarządzania konfiguracją i energią (ACPI) przycisk zasilania komputera może działać jako włącznik/wyłącznik zasilania lub jako przycisk wstrzymania. Działanie funkcji wstrzymania polega na tym, że komputer nie jest zupełnie wyłączany, ale wprowadzany w stan niskiego poboru energii. Pozwala to na szybkie zmniejszenie zużycia energii (przejście do trybu oszczędzania energii) bez konieczności zamykania programów, a także szybki powrót do tego samego stanu bez ryzyka utraty danych.

Aby zmienić sposób działania przycisku zasilania, wykonaj następujące czynności:

1. W systemie Windows 2000 kliknij przycisk **Start**, a następnie wybierz kolejno **Ustawienia > Panel sterowania > Opcje zasilania**.

   W systemach Windows XP Professional i Home Edition kliknij przycisk **Start**, a następnie wybierz kolejno **Panel sterowania > Wydajność i konserwacja > Opcje zasilania**.

2. W oknie **Właściwości: Opcje zasilania** wybierz kartę **Zaawansowane**.

3. W obszarze **Przycisk zasilania** wybierz żądane ustawienie przycisku zasilania.

Po skonfigurowaniu przycisku zasilania jako przycisku wstrzymania jego naciśnięcie spowoduje przejście systemu w stan niskiego poboru energii (stan wstrzymania). Ponowne jego naciśnięcie spowoduje natomiast szybkie uaktywnienie systemu i przejście komputera do trybu pełnego zasilania. Aby całkowicie wyłączyć komputer, należy nacisnąć przycisk zasilania i przytrzymać go w tej pozycji przez kilka sekund.

PRZESTROGA: Przycisku zasilania należy używać do wyłączania komputera tylko w przypadku braku odpowiedzi systemu. Wyłączanie zasilania bez interakcji ze strony systemu operacyjnego może doprowadzić do uszkodzenia lub utraty danych zgromadzonych na dysku twardym.

Witryna internetowa

Personel techniczny firmy HP na bieżąco testuje i usuwa błędy w programach własnych oraz dostarczanych przez innych producentów, jak również prowadzi prace nad oprogramowaniem wspomagającym, przeznaczonym dla różnych systemów operacyjnych. Zapewnia to wydajność, zgodność i niezawodność komputerów firmy HP.

Wskazane jest, aby podczas zmiany lub uaktualniania systemów operacyjnych zaimplementować zaprojektowane dla nich oprogramowanie wspomagające. Jeśli planowane jest korzystanie z wersji systemu Microsoft Windows innej niż zainstalowana fabrycznie, należy zainstalować odpowiednie sterowniki urządzeń oraz programy narzędziowe (dzięki temu wszystkie dostępne funkcje będą realizowane poprawnie).

Dzięki staraniom firmy HP procesy odnajdywania, uzyskiwania dostępu, uaktualniania i instalowania najnowszego oprogramowania wspomagającego są bardzo proste. Oprogramowanie można pobrać ze witryny http://www.hp.com/support.

W witrynie tej dostępne są najnowsze wersje sterowników urządzeń, programy narzędziowe oraz możliwe do aktualizowania obrazy pamięci ROM, niezbędne do pracy najnowszej wersji systemu Windows na komputerach firmy HP.

Współpraca z innymi producentami

Opracowane przez firmę HP rozwiązania do zarządzania integrują się z innymi aplikacjami do zarządzania systemem i są oparte na standardach przemysłowych, takich jak:

- Desktop Management Interface (DMI) 2.0
- Technologia Wake on LAN
- ACPI
- SMBIOS
- Środowisko Pre-boot Execution (PXE)

Śledzenie zasobów i funkcje zabezpieczeń

Komputery firmy HP są wyposażone w funkcje śledzenia zasobów. Zgromadzone dane dotyczące stanu kluczowych zasobów mogą być przetwarzane za pomocą oprogramowania HP Insight Manager, HP Client Manager lub innych aplikacji do zarządzania systemem. Ze względu na całkowitą i automatyczną integrację funkcji śledzenia zasobów ze wspomnianymi programami, użytkownik może wybrać narzędzie do zarządzania najlepiej odpowiadające jego środowisku pracy oraz podnoszące efektywność już używanego oprogramowania narzędziowego.

Firma HP oferuje również kilka rozwiązań służących do kontroli dostępu do cennych podzespołów i informacji. Wbudowany mikroukład zabezpieczeń ProtectTools Embedded Security (po zainstalowaniu) zapobiega nieautoryzowanemu dostępowi do danych, a także sprawdza integralność systemu i uwierzytelnia innych użytkowników próbujących uzyskać dostęp do systemu. Dostępne w wybranych modelach funkcje zabezpieczeń, takie jak ProtectTools, blokada Smart Cover Lock i czujnik Smart Cover Sensor, zapobiegają nieautoryzowanemu dostępowi do wewnętrznych podzespołów komputera. Z kolei wyłączając porty szeregowe, równoległe lub USB albo wyłączając możliwość uruchamiania systemu z nośników wymiennych, można chronić cenne dane. Alerty dotyczące zmiany rozmiaru pamięci oraz otworzenia obudowy mogą być automatycznie przesyłane do aplikacji zarządzania systemem, przez co będą pełniły funkcję proaktywnego powiadamiania o ingerencji w wewnętrzne elementy komputera.

Pakiet Protect Tools, czujnik Smart Cover Sensor i blokada Smart Cover Lock są dostępne jako opcje w niektórych systemach.

Ustawienia zabezpieczeń komputerów firmy HP mogą być zarządzane na dwa sposoby:

- Lokalnie, za pomocą oprogramowania narzędziowego Computer Setup. Dodatkowe informacje i instrukcje dotyczące korzystania z programu Computer Setup można znaleźć w *Podręczniku do programu Computer Setup (F10)* dołączonym do komputera.

- Zdalnie, za pomocą programu HP Client Manager lub System Software Manager, umożliwiającego bezpieczne rozmieszczanie i kontrolowanie jednolitych ustawień zabezpieczeń z poziomu prostego narzędzia wiersza polecenia.

Poniższa tabela oraz dalsze części dotyczą lokalnego zarządzania funkcjami zabezpieczeń komputera za pomocą oprogramowania narzędziowego Computer Setup (F10).

Przegląd funkcji zabezpieczeń

Funkcja	Zastosowanie	Sposób ustawiania
Kontrola uruchamiania systemu z nośników wymiennych	Zapobiega uruchamianiu systemu z nośników wymiennych. (Funkcja dostępna w wybranych modelach).	W menu oprogramowania Computer Setup (F10)
Kontrola interfejsu szeregowego, równoległego, USB lub portu podczerwieni	Zapobiega transferowi danych za pośrednictwem zintegrowanego interfejsu szeregowego, równoległego, USB (universal serial bus) lub portu podczerwieni.	W menu oprogramowania Computer Setup (F10)
Hasło uruchomieniowe	Uniemożliwia uruchomienie komputera bez podania poprawnego hasła. Dotyczy to zarówno pierwszego, jak i ponownych uruchomień komputera.	W menu oprogramowania Computer Setup (F10)
Hasło konfiguracyjne	Uniemożliwia zmianę ustawień konfiguracyjnych komputera (za pomocą oprogramowania Computer Setup) bez podania poprawnego hasła.	W menu oprogramowania Computer Setup (F10)

Więcej informacji o programie Computer Setup znajduje się w *Podręczniku do programu Computer Setup (F10)*.

Obsługa opcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.

Przegląd funkcji zabezpieczeń *(ciąg dalszy)*

Funkcja	Zastosowanie	Sposób ustawiania
Wbudowany mikroukład zabezpieczeń	Zapobiega nieautoryzowanemu dostępowi do danych, używając ochrony za pomocą szyfrowania i haseł. Sprawdza integralność systemu i uwierzytelnia innych użytkowników próbujących uzyskać dostęp do systemu.	W menu oprogramowania Computer Setup (F10)
Funkcja DriveLock	Zapobiega nieautoryzowanemu dostępowi do danych przechowywanych na dyskach twardych MultiBay. Funkcja ta jest dostępna jedynie w niektórych modelach.	W menu oprogramowania Computer Setup (F10)
Czujnik Smart Cover Sensor	Informuje o zdjęciu obudowy lub panelu bocznego komputera. Odpowiednie ustawienie tej funkcji umożliwia uruchamianie komputera ze zdjętą obudową tylko po wprowadzeniu hasła konfiguracyjnego. Więcej informacji o tej funkcji można znaleźć w *Instrukcji obsługi sprzętu* na dysku CD *Biblioteka z dokumentacją*. Funkcja ta jest dostępna jedynie w niektórych modelach.	W menu oprogramowania Computer Setup (F10)

Więcej informacji o programie Computer Setup znajduje się w *Podręczniku do programu Computer Setup (F10)*.

Obsługa opcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.

Przegląd funkcji zabezpieczeń *(ciąg dalszy)*

Funkcja	Zastosowanie	Sposób ustawiania
Zabezpieczenie głównego rekordu rozruchowego	Umożliwia cofnięcie wprowadzonych przypadkowo lub celowo zmian głównego rekordu rozruchowego (MBR) bieżącego dysku rozruchowego. Wersja tego rekordu, przy której nastąpiło ostatnie poprawne uruchomienie systemu, jest rejestrowana i w razie konieczności może zostać odzyskana.	W menu oprogramowania Computer Setup (F10)
Alerty dotyczące zmiany rozmiaru pamięci	Pojawiają się po dodaniu, przeniesieniu lub usunięciu modułów pamięci. Są przesyłane do użytkownika oraz do administratora systemu.	Informacje na temat uaktywniania funkcji alertów dotyczących zmiany rozmiaru pamięci można uzyskać w dostępnym online podręczniku *Intelligent Manageability Guide*.

Więcej informacji o programie Computer Setup znajduje się w *Podręczniku do programu Computer Setup (F10)*.

Obsługa opcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.

Przegląd funkcji zabezpieczeń *(ciąg dalszy)*

Funkcja	Zastosowanie	Sposób ustawiania
Etykieta właściciela	Wyświetla podczas uruchamiania systemu etykietę właściciela komputera, zdefiniowaną przez administratora systemu (funkcja chroniona hasłem konfiguracyjnym).	W menu oprogramowania Computer Setup (F10)
Zabezpieczająca blokada kablowa	Blokuje dostęp do wnętrza komputera, a tym samym zapobiega niepożądanym wymianom oraz usuwaniu podzespołów wewnętrznych. Zabezpieczenie to pozwala również na przymocowanie komputera do nieruchomego obiektu w celu uniemożliwienia jego kradzieży.	Zainstalowanie blokady kablowej w celu przymocowania komputera do nieruchomego obiektu.
Blokada z pętlą zabezpieczającą	Blokuje dostęp do wnętrza komputera, a tym samym zapobiega niepożądanym wymianom oraz usuwaniu podzespołów wewnętrznych.	Zainstalowanie blokady w pętli zabezpieczającej w celu uniemożliwienia wymiany oraz usuwania podzespołów wewnętrznych przez osoby nieupoważnione.

Więcej informacji o programie Computer Setup znajduje się w *Podręczniku do programu Computer Setup (F10)*.

Obsługa opcji zabezpieczeń może się różnić w zależności od konfiguracji komputera.

Zabezpieczanie hasłem

Hasło uruchomieniowe zapobiega nieautoryzowanemu dostępowi do komputera. Jego podanie jest wymagane przy każdorazowym włączaniu lub ponownym uruchamianiu komputera.
Hasło konfiguracyjne zapobiega nieautoryzowanemu dostępowi do programu Computer Setup. Można go również używać jako hasła uruchomieniowego. Oznacza to, że podanie hasła konfiguracyjnego zamiast uruchomieniowego umożliwi uzyskanie dostępu do zasobów komputera.

Administrator systemu może dysponować hasłem konfiguracyjnym obowiązującym w całej sieci. Dzięki niemu ma on dostęp do wszystkich komputerów oraz możliwość sprawowania kontroli nad działaniem całego systemu, nawet jeżeli stanowiska są chronione za pomocą haseł uruchomieniowych.

Ustawianie hasła konfiguracyjnego za pomocą programu Computer Setup

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w części „Wbudowany mikroukład zabezpieczeń” na stronie 33.

Ustawienie hasła konfiguracyjnego za pomocą programu Computer Setup zapobiega przypadkowym i nieautoryzowanym zmianom konfiguracji komputera, gdyż dostęp do programu Computer Setup (F10) będzie możliwy wyłącznie po podaniu hasła.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

3. Wybierz menu **Security (Zabezpieczenia)**, wybierz opcję **Setup Password (Hasło konfiguracyjne)**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

Ustawianie hasła uruchomieniowego za pomocą programu Computer Setup

Po ustawieniu hasła uruchomieniowego za pomocą programu Computer Setup dostęp do danych komputera jest możliwy dopiero po podaniu poprawnego hasła. Ustawienie tego hasła spowoduje również wyświetlenie w menu Security (Zabezpieczenia) programu Computer Setup pozycji Password Options (Opcje hasła). Do opcji hasła należy Password Prompt on Warm Boot (Wymaganie hasła przy ponownym uruchamianiu). Jeżeli włączona zostanie opcja wymagania hasła przy ponownym uruchamianiu, wprowadzanie hasła będzie konieczne również przy każdym ponownym uruchomieniu komputera.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

---

3. Wybierz menu **Security (Zabezpieczenia)**, wybierz opcję **Power-On Password (Hasło uruchomieniowe)**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

Wprowadzanie hasła uruchomieniowego

Aby wprowadzić hasło uruchomieniowe, wykonaj następujące czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Po pojawieniu się ikony klucza wpisz bieżące hasło, a następnie naciśnij klawisz **Enter**.

Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

Jeżeli zostanie podane nieprawidłowe hasło, na ekranie pojawi się ikona przedstawiająca przełamany klucz. Należy spróbować ponowne wpisać poprawne hasło. Po trzech nieudanych próbach wprowadzenia hasła komputer należy wyłączyć, a następnie włączyć i ponownie wprowadzić hasło.

Wprowadzanie hasła konfiguracyjnego

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w części „Wbudowany mikroukład zabezpieczeń” na stronie 33.

Jeżeli ustawiono hasło konfiguracyjne komputera, jego podanie będzie wymagane przy każdej próbie uruchomienia programu Computer Setup.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

3. Po pojawieniu się ikony klucza wpisz hasło konfiguracyjne, a następnie naciśnij klawisz **Enter**.

Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

Jeżeli zostanie podane nieprawidłowe hasło, na ekranie pojawi się ikona przedstawiająca przełamany klucz. Należy spróbować ponowne wpisać poprawne hasło. Po trzech nieudanych próbach wprowadzenia hasła komputer należy wyłączyć, a następnie włączyć i ponownie wprowadzić hasło.

Zmiana hasła uruchomieniowego lub konfiguracyjnego

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w części „Wbudowany mikroukład zabezpieczeń” na stronie 33.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**. Aby zmienić hasło konfiguracyjne, uruchom program **Computer Setup**.
2. Po pojawieniu się ikony klucza wpisz bieżące hasło, a następnie dwa razy nowe hasło, rozdzielając je znakiem ukośnika (/) lub innym separatorem, zgodnie ze wzorem:
   bieżące hasło/nowe hasło/nowe hasło

Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

3. Naciśnij klawisz **Enter**.

Nowe hasło zacznie obowiązywać po następnym włączeniu komputera.

Informacje na temat innych separatorów można znaleźć w części „Separatory dla różnych układów klawiatury” na stronie 32. Hasła uruchomieniowe i konfiguracyjne można również zmieniać przy użyciu opcji menu Security (Zabezpieczenia) w programie Computer Setup.

Usuwanie hasła uruchomieniowego lub konfiguracyjnego

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w części „Wbudowany mikroukład zabezpieczeń” na stronie 33.

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**. Aby usunąć hasło konfiguracyjne, uruchom program **Computer Setup**.
2. Po pojawieniu się ikony klucza wpisz bieżące hasło, a następnie znak ukośnika (/) lub inny separator, zgodnie ze wzorem: **bieżące hasło/**
3. Naciśnij klawisz **Enter**.

Informacje na temat innych separatorów można znaleźć w części „Separatory dla różnych układów klawiatury”.
Hasła uruchomieniowe i konfiguracyjne można również zmieniać przy użyciu opcji menu Security (Zabezpieczenia) w programie Computer Setup.

Separatory dla różnych układów klawiatury

Konstrukcja każdej klawiatury uwzględnia wymagania specyficzne dla danego języka. Z tego względu separatory oraz klawisze używane podczas zmiany lub usuwania hasła zależą od typu klawiatury dołączonej do komputera.

Separatory dla różnych układów klawiatury

angielska (USA)	/	francuska (Kanada)	é	portugalska	-
angielska (Wielka Brytania)	/	grecka	-	rosyjska	/
arabska	/	hebrajska		słowacka	-
belgijska	=	hiszpańska	-	szwajcarska	-
BHCSY*	-	japońska	/	szwedzka/ fińska	/
brazylijska	/	koreańska	/	tajska	/

Separatory dla różnych układów klawiatury

chińska	/	niemiecka	-	tajwańska	/
czeska	-	norweska	-	turecka	.
duńska	-	południowo-amerykańska	-	włoska	-
francuska	!	polska	-	węgierska	-

* dotyczy Bośni-Hercegowiny, Chorwacji, Słowenii i Jugosławii

Czyszczenie haseł

Utrata hasła uniemożliwia dostęp do komputera. W *Podręczniku rozwiązywania problemów* można znaleźć instrukcje dotyczące czyszczenia haseł.

Jeśli system jest wyposażony we wbudowany mikroukład zabezpieczeń, należy zapoznać się z informacjami w części „Wbudowany mikroukład zabezpieczeń”.

Wbudowany mikroukład zabezpieczeń

Wbudowany mikroukład zabezpieczeń ProtectTools Embedded Security łączy w sobie funkcje szyfrowania i ochrony hasłem w celu zapewnienia maksymalnego bezpieczeństwa danych podczas szyfrowania plików/folderów systemu plików EFS (Embedded File System), a także zabezpieczenia wiadomości e-mail przesyłanych przy użyciu programów Microsoft Outlook i Outlook Express. Narzędzie ProtectTools jest dostępne w wybranych komputerach typu Business Desktop jako opcja konfiguracji na zamówienie (Configured-To-Order — CTO). Opracowano je z myślą o klientach firmy HP, dla których bezpieczeństwo danych jest sprawą priorytetową: utrata danych stanowi nieporównywalnie mniejsze niebezpieczeństwo niż uzyskanie dostępu do nich przez osoby nieupoważnione. Narzędzie ProtectTools używa czterech haseł:

- (F10) Setup — służy do uruchamiania programu Computer Setup (F10) oraz do włączania/wyłączania narzędzia ProtectTools.
- Take Ownership (Przejęcie na własność) — hasło ustawiane i używane przez administratora systemu, który będzie autoryzować użytkowników i określać parametry zabezpieczeń.

- Emergency Recovery Token (Token odzyskiwania danych po awarii) — hasło ustawiane przez administratora, umożliwia odzyskiwanie danych w przypadku awarii komputera lub mikroukładu ProtectTools.
- Basic User (Użytkownik końcowy) — hasło ustawiane i używane przez użytkownika końcowego.

W przypadku utraty hasła użytkownika końcowego odzyskanie zaszyfrowanych danych jest niemożliwe. Dlatego też w celu zwiększenia bezpieczeństwa związanego ze stosowaniem narzędzia ProtectTools zalecane jest regularne tworzenie kopii zapasowych danych przechowywanych na dysku użytkownika lub replikowanie ich w systemie informacyjnym.

Wbudowany mikroukład zabezpieczeń ProtectTools Embedded Security jest zgodny ze standardem TCPA 1.1 i jest opcjonalnie instalowany na płytach głównych wybranych komputerów Busines Desktop. Każdy wbudowany mikroukład zabezpieczeń ProtectTools Embedded Security jest unikatowy i powiązany z określonym komputerem. Każdy mikroukład przeprowadza kluczowe procesy zabezpieczeń niezależnie od innych elementów komputera (np. procesor, pamięć lub system operacyjny).

Wbudowany mikroukład zabezpieczeń ProtectTools Embedded Security uzupełnia i zwiększa możliwości zabezpieczeń komputera, które wchodzą w skład systemu Microsoft Windows 2000, Windows XP Professional lub Home Edition. Na przykład system operacyjny może szyfrować lokalne pliki i foldery systemu EFS, natomiast wbudowany mikroukład zabezpieczeń ProtectTools Embedded Security oferuje dodatkową warstwę zabezpieczeń, tworząc klucze szyfrowania na podstawie głównego klucza platformy (zapisanego w krzemowym układzie scalonym). Ten proces jest znany jako „wrapping” (opakowywanie) kluczy szyfrowania. Narzędzie ProtectTools nie zabezpiecza przed dostępem poprzez sieć komputera bez tego narzędzia.

Do najważniejszych funkcji wbudowanego mikroukładu zabezpieczeń ProtectTools Embedded Security należą:

- Uwierzytelnianie platformy
- Chroniony magazyn
- Integralność danych

PRZESTROGA: Hasła należy zabezpieczyć. **Bez haseł nie jest możliwy dostęp do zaszyfrowanych danych ani ich odzyskanie**.

Ustawianie haseł

Program Setup

Przy użyciu narzędzia konfiguracyjnego F10 można tworzyć hasło konfiguracyjne i włączać wbudowany mikroukład zabezpieczeń.

1. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

2. Za pomocą klawisza ze strzałką w górę lub w dół wybierz język, a następnie naciśnij klawisz **Enter**.
3. Za pomocą klawisza ze strzałką w lewo lub w prawo przejdź do karty **Security (Zabezpieczenia)**, a następnie, używając klawiszy ze strzałkami w górę lub w dół, przejdź do opcji **Setup Password (Hasło konfiguracyjne)**. Naciśnij klawisz **Enter**.
4. Wpisz hasło i potwierdź je. Naciśnij klawisz **F10**, aby zaakceptować hasło.

Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

5. Za pomocą klawisza ze strzałką w górę lub w dół przejdź do opcji **Embedded Security Device (Wbudowany mikroukład zabezpieczeń)**. Naciśnij klawisz **Enter**.
6. Jeśli w oknie dialogowym jest wybrana opcja **Embedded Security Device — Disable (Wbudowany mikroukład zabezpieczeń — Wyłącz)**, za pomocą klawiszy ze strzałką w lewo lub w prawo zmień ją na **Embedded Security Device — Enable (Wbudowany mikroukład zabezpieczeń — Włącz)**. Naciśnij klawisz **F10**, aby zaakceptować zmianę.

PRZESTROGA: Wybranie opcji **Reset to Factory Settings — Reset (Przywróć ustawienia fabryczne — Przywróć)** powoduje wyczyszczenie wszystkich kluczy i zaszyfrowane dane staną się niemożliwe do odzyskania, *chyba że* utworzono kopie zapasowe tych kluczy (zobacz „Przejęcie na własność i token odzyskiwania danych po awarii"). Polecenia **Reset (Przywróć)** należy używać tylko w przypadku pojawienia się takiego zalecenia podczas odzyskiwania zaszyfrowanych danych (zobacz „Odzyskiwanie zaszyfrowanych danych" na stronie 39).

7. Za pomocą klawisza ze strzałką w lewo lub w prawo przejdź do menu **File (Plik)**. Za pomocą klawisza ze strzałką w górę lub w dół przejdź do polecenia **Save Changes and Exit (Zapisz zmiany i zakończ)**. Naciśnij klawisz **Enter**, a następnie klawisz **F10** w celu potwierdzenia zmian.

Przejęcie na własność i token odzyskiwania danych po awarii

Hasło Take Ownership (Przejęcie na własność) jest wymagane do włączania lub wyłączania platformy zabezpieczeń oraz do autoryzowania użytkowników. W przypadku awarii wbudowanego mikroukładu zabezpieczeń mechanizm odzyskiwania danych po awarii umożliwia autoryzowanie użytkowników oraz dostęp do danych.

1. Jeśli używany jest system Windows XP Professional lub Home Edition, kliknij kolejno **Start > Wszystkie programy > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

   Jeśli używany jest system Windows 2000, kliknij kolejno **Start > Programy > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

2. Kliknij przycisk **Next (Dalej)**.
3. Wprowadź i potwierdź hasło Take Ownership (Przejęcie na własność), a następnie kliknij przycisk **Next (Dalej)**.

Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

4. Kliknij przycisk **Next (Dalej)**, aby zaakceptować domyślną lokalizację archiwum odzyskiwania danych.
5. Wprowadź i potwierdź hasło Emergency Recovery Token (Token odzyskiwania danych po awarii), a następnie kliknij przycisk **Next (Dalej)**.
6. Włóż dyskietkę, na której ma zostać zapisany klucz tokenu odzyskiwania danych po awarii. Kliknij przycisk **Browse (Przeglądaj)** i wybierz dyskietkę.

PRZESTROGA: Klucz tokenu odzyskiwania danych po awarii służy do odzyskiwania zaszyfrowanych danych w przypadku wystąpienia awarii komputera lub wbudowanego mikroukładu zabezpieczeń. **Odzyskanie danych bez podania klucza jest niemożliwe**. (W dalszym ciągu dostęp do danych można uzyskać dopiero po podaniu hasła użytkownika końcowego). Dyskietkę należy przechowywać w bezpiecznym miejscu.

7. Kliknij przycisk **Save (Zapisz)**, aby zaakceptować lokalizację i domyślną nazwę pliku, a następnie kliknij przycisk **Next (Dalej)**.
8. Kliknij przycisk **Next (Dalej)**, aby potwierdzić ustawienia przed zainicjowaniem platformy zabezpieczeń.

Może pojawić się komunikat informujący, że funkcje wbudowanego mikroukładu zabezpieczeń nie zostały zainicjowane. Nie należy klikać okna tego komunikatu; istnieje do niego odwołanie w dalszej części procedury. Okno zostanie zamknięte po kilku sekundach.

9. Kliknij przycisk **Next (Dalej)**, aby pominąć etap konfigurowania zasad lokalnych.
10. Sprawdź, czy zostało zaznaczone pole wyboru Start Embedded Security User Initialization Wizard (Uruchom kreatora inicjowania użytkownika wbudowanego mikroukładu zabezpieczeń), a następnie kliknij przycisk **Finish (Zakończ)**.

Kreator inicjowania użytkownika wbudowanego mikroukładu zabezpieczeń zostanie uruchomiony automatycznie.

Hasło użytkownika końcowego

Podczas inicjowania użytkownika tworzone jest hasło użytkownika końcowego (Basic User). Jest ono wymagane do wprowadzania zaszyfrowanych danych oraz uzyskiwania do nich dostępu.

PRZESTROGA: Należy zabezpieczyć hasło użytkownika końcowego. **Bez tego hasła nie jest możliwy dostęp do zaszyfrowanych danych ani ich odzyskanie**.

1. Jeśli nie jest uruchomiony Kreator inicjowania użytkownika:

   Jeśli używany jest system Windows XP Professional lub Home Edition, kliknij kolejno **Start > Wszystkie programy > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

   Jeśli używany jest system Windows 2000, kliknij kolejno **Start > Programy > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.
2. Kliknij przycisk **Next (Dalej)**.
3. Wprowadź i potwierdź hasło Basic User Key (Klucz użytkownika końcowego), a następnie kliknij przycisk **Next (Dalej)**.

Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

4. Kliknij przycisk **Next (Dalej)**, aby potwierdzić ustawienia.
5. Wybierz odpowiednie funkcje zabezpieczeń i kliknij przycisk **Next (Dalej)**.
6. Kliknij odpowiedniego klienta poczty e-mail, a następnie kliknij przycisk **Next (Dalej)**.
7. Kliknij przycisk **Next (Dalej)**, aby zastosować certyfikat szyfrowania.
8. Kliknij przycisk **Next (Dalej)**, aby potwierdzić ustawienia.
9. Kliknij przycisk **Finish (Zakończ)**.
10. Uruchom ponownie komputer.

Odzyskiwanie zaszyfrowanych danych

Aby możliwe było odzyskanie danych po wymianie mikroukładu ProtectTools, wymagane jest posiadanie następujących elementów:

- SPEmRecToken.xml — klucz tokenu odzyskiwania danych po awarii
- SPEmRecArchive.xml — folder ukryty, domyślna lokalizacja: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- Hasła ProtectTools
  - Hasło konfiguracyjne
  - Hasło przejęcia na własność
  - Token odzyskiwania danych po awarii
  - Hasło użytkownika końcowego

1. Uruchom ponownie komputer.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

3. Wprowadź hasło konfiguracyjne i naciśnij klawisz **Enter**.
4. Za pomocą klawisza ze strzałką w górę lub w dół wybierz język, a następnie naciśnij klawisz **Enter**.
5. Za pomocą klawisza ze strzałką w lewo lub w prawo przejdź do karty **Security (Zabezpieczenia)**, a następnie, używając klawisza ze strzałką w górę lub w dół, przejdź do opcji **Embedded Security Device (Wbudowany mikroukład zabezpieczeń)**. Naciśnij klawisz **Enter**.
6. Jeśli dostępna jest tylko jedna opcja **Embedded Security Device — Disable (Wbudowany mikroukład zabezpieczeń — Wyłącz)**:

   a. Za pomocą klawisza ze strzałką w lewo lub w prawo zmień ustawienie tej opcji na **Embedded Security Device — Enable (Wbudowany mikroukład zabezpieczeń — Włącz)**. Naciśnij klawisz **F10**, aby zaakceptować zmianę.

   b. Za pomocą klawisza ze strzałką w lewo lub w prawo przejdź do menu **File (Plik)**. Za pomocą klawisza ze strzałką w górę lub w dół przejdź do polecenia **Save Changes and Exit (Zapisz zmiany i zakończ)**. Naciśnij klawisz **Enter**, a następnie klawisz **F10** w celu potwierdzenia zmian.

   c. Przejdź do punktu 1.

   Jeśli dostępne są dwie opcje, przejdź do punku 7.

7. Za pomocą klawisza ze strzałką w górę lub w dół przejdź do opcji **Reset to Factory Settings — Do Not Reset (Przywróć ustawienia fabryczne — Nie przywracaj)**. Naciśnij jeden raz klawisz ze strzałką w lewo lub w prawo.

   Zostanie wyświetlony komunikat: Performing this action will reset the embedded security device to factory settings if settings are saved on exit. Press any key to continue. (Wykonanie tej czynności spowoduje zresetowanie wbudowanego mikroukładu zabezpieczeń do ustawień fabrycznych, jeżeli ustawienia zostaną zapisane przy wyjściu. Naciśnij dowolny klawisz, aby kontynuować).

   Naciśnij klawisz **Enter**.

8. Ustawienie ulegnie zmianie na **Reset to Factory Settings — Reset (Przywróć ustawienia fabryczne — Przywróć)**. Naciśnij klawisz **F10**, aby zaakceptować zmianę.
9. Za pomocą klawisza ze strzałką w lewo lub w prawo przejdź do menu **File (Plik)**. Za pomocą klawisza ze strzałką w górę lub w dół przejdź do polecenia **Save Changes and Exit (Zapisz zmiany i zakończ)**. Naciśnij klawisz **Enter**, a następnie klawisz **F10** w celu potwierdzenia zmian.
10. Uruchom ponownie komputer.
11. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

---

12. Wpisz hasło konfiguracyjne i naciśnij klawisz **Enter**.
13. Za pomocą klawisza ze strzałką w górę lub w dół wybierz język, a następnie naciśnij klawisz **Enter**.
14. Za pomocą klawisza ze strzałką w lewo lub w prawo przejdź do karty **Security (Zabezpieczenia)**, a następnie, używając klawisza ze strzałką w górę lub w dół, przejdź do opcji **Embedded Security Device (Wbudowany mikroukład zabezpieczeń)**. Naciśnij klawisz **Enter**.
15. Jeśli w oknie dialogowym jest wybrana opcja **Embedded Security Device — Disable (Wbudowany mikroukład zabezpieczeń — Wyłącz)**, za pomocą klawisza ze strzałką w lewo lub w prawo zmień ją na **Embedded Security Device — Enable (Wbudowany mikroukład zabezpieczeń — Włącz)**. Naciśnij klawisz **F10**.
16. Za pomocą klawisza ze strzałką w lewo lub w prawo przejdź do menu **File (Plik)**. Za pomocą klawisza ze strzałką w górę lub w dół przejdź do polecenia **Save Changes and Exit (Zapisz zmiany i zakończ)**. Naciśnij klawisz **Enter**, a następnie klawisz **F10** w celu potwierdzenia zmian.

17. Po otwarciu systemu Windows:

    Jeśli używany jest system Windows XP Professional lub Home Edition, kliknij kolejno **Start > Wszystkie programy > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

    Jeśli używany jest system Windows 2000, kliknij kolejno **Start > Programy > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

18. Kliknij przycisk **Next (Dalej)**.
19. Wprowadź i potwierdź hasło Take Ownership (Przejęcie na własność). Kliknij przycisk **Next (Dalej)**.

Hasło należy wpisywać uważnie, ponieważ ze względów bezpieczeństwa znaki nie są wyświetlane na ekranie.

20. Sprawdź, czy została wybrana opcja tworzenia nowego archiwum odzyskiwania danych. W obszarze **Recovery archive location (Lokalizacja archiwum odzyskiwania danych)** kliknij przycisk **Browse (Przeglądaj)**.
21. Nie akceptuj domyślnej nazwy pliku. Wpisz nową nazwę, aby uniknąć zastąpienia pliku pierwotnego.
22. Kliknij przycisk **Save (Zapisz)**, a następnie przycisk **Next (Dalej)**.
23. Wprowadź i potwierdź hasło Emergency Recovery Token (Token odzyskiwania danych po awarii), a następnie kliknij przycisk **Next (Dalej)**.
24. Włóż dyskietkę, na której ma zostać zapisany klucz tokenu odzyskiwania danych po awarii. Kliknij przycisk **Browse (Przeglądaj)** i wybierz dyskietkę.
25. Nie akceptuj domyślnej nazwy klucza. Wpisz nową nazwę, aby uniknąć zastąpienia klucza pierwotnego.
26. Kliknij przycisk **Save (Zapisz)**, a następnie przycisk **Next (Dalej)**.
27. Kliknij przycisk **Next (Dalej)**, aby potwierdzić ustawienia przed zainicjowaniem platformy zabezpieczeń.

Może pojawić się komunikat informujący, że nie można załadować klucza użytkownika końcowego. Nie należy klikać okna tego komunikatu; istnieje do niego odwołanie w dalszej części procedury. Okno zostanie zamknięte po kilku sekundach.

28. Kliknij przycisk **Next (Dalej)**, aby pominąć etap konfigurowania zasad lokalnych.
29. Usuń zaznaczenie pola wyboru **Start Embedded Security User Initialization Wizard (Uruchom kreatora inicjowania użytkownika wbudowanego mikroukładu zabezpieczeń)**. Kliknij przycisk **Finish (Zakończ)**.
30. Kliknij prawym przyciskiem myszy ikonę ProtectTools na pasku narzędzi, a następnie kliknij polecenie **Initialize Embedded Security restoration (Zainicjuj przywracanie wbudowanego mikroukładu zabezpieczeń)**.

    Spowoduje to uruchomienie kreatora HP ProtectTools Embedded Security Initialization Wizard.
31. Kliknij przycisk **Next (Dalej)**.
32. Włóż dyskietkę, na której jest zapisany pierwotny klucz tokenu odzyskiwania danych po awarii. Kliknij przycisk **Browse (Przeglądaj)**, a następnie znajdź i kliknij dwukrotnie token w celu wprowadzenia nazwy w polu. Domyślna nazwa to A:\SPEmRecToken.xml.
33. Wprowadź pierwotne hasło tokenu i kliknij przycisk **Next (Dalej)**.
34. Kliknij przycisk **Browse (Przeglądaj)**, a następnie znajdź i kliknij dwukrotnie pierwotne archiwum odzyskiwania danych w celu wprowadzenia nazwy w polu. Nazwa domyślna to C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Kliknij przycisk **Next (Dalej)**.
36. Kliknij komputer, który ma zostać odzyskany, a następnie kliknij przycisk **Next (Dalej)**.
37. Kliknij przycisk **Next (Dalej)**, aby potwierdzić ustawienia.

38. Jeśli zostanie wyświetlony komunikat o przywróceniu platformy zabezpieczeń, przejdź do punktu 39.

    W przeciwnym wypadku wróć do punktu 10. Sprawdź uważnie hasła, nazwę i lokalizację tokenu oraz nazwę i lokalizację archiwum.

39. Kliknij przycisk Finish (Zakończ).

40. Jeśli używany jest system Windows XP Professional lub Home Edition, kliknij kolejno **Start > Wszystkie programy > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

    Jeśli używany jest system Windows 2000, kliknij kolejno **Start > Programy > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

41. Kliknij przycisk **Next (Dalej)**.

42. Kliknij opcję **Recover your basic user key (Odzyskaj klucz użytkownika końcowego)**, a następnie kliknij przycisk **Next (Dalej)**.

43. Wybierz użytkownika, wpisz hasło Basic User Key (Klucz użytkownika końcowego), a następnie kliknij przycisk **Next (Dalej)**.

44. Kliknij przycisk **Next (Dalej)**, aby potwierdzić ustawienia i zaakceptować domyślną lokalizację danych dotyczących odzyskiwania.

Wykonanie czynności z punktów od 45 do 49 powoduje ponowne zainstalowanie pierwotnej konfiguracji hasła użytkownika końcowego.

---

45. Wybierz odpowiednie funkcje zabezpieczeń i kliknij przycisk **Next (Dalej)**.

46. Kliknij odpowiedniego klienta poczty e-mail, a następnie kliknij przycisk **Next (Dalej)**.

47. Kliknij certyfikat szyfrowania, a następnie kliknij przycisk **Next (Dalej)**, aby go zastosować.

48. Kliknij przycisk **Next (Dalej)**, aby potwierdzić ustawienia.

49. Kliknij przycisk **Finish (Zakończ)**.
50. Uruchom ponownie komputer.

PRZESTROGA: Należy zabezpieczyć hasło użytkownika końcowego. **Bez tego hasła nie jest możliwy dostęp do zaszyfrowanych danych ani ich odzyskanie**.

Funkcja DriveLock

DriveLock to będąca standardem przemysłowym funkcja zabezpieczeń, która zapobiega nieautoryzowanemu dostępowi do danych przechowywanych na dyskach twardych MultiBay. Funkcja ta jest zaimplementowana jako rozszerzenie programu Computer Setup. Jest ona dostępna tylko po wykryciu w systemie dysku twardego z obsługą funkcji DriveLock.

Funkcja DriveLock została opracowana z myślą o klientach firmy HP, dla których bezpieczeństwo danych jest sprawą priorytetową. Chodzi o klientów, dla których całkowity koszt dysku twardego i danych na nim przechowywanych (w przypadku ich utraty) jest nieporównanie mniejszy od strat, jakie może spowodować dostęp do tych danych przez osoby niepowołane. W celu uzyskania kompromisu między wymaganym poziomem zabezpieczeń i koniecznością dostępu do danych w przypadku utraty hasła implementacja funkcji DriveLock wykorzystuje schemat zabezpieczeń oparty na dwóch hasłach. Pierwsze z nich jest ustawiane i stosowane przez administratora systemu, drugie natomiast — przez użytkownika końcowego. Jeżeli oba hasła zostaną utracone, dostęp do dysku zostanie całkowicie zablokowany. Dlatego też w celu zwiększenia bezpieczeństwa związanego ze stosowaniem funkcji DriveLock zalecane jest replikowanie lub tworzenie kopii zapasowych danych przechowywanych na dysku w wewnętrznym systemie informacyjnym przedsiębiorstwa.

W przypadku utraty obu haseł używanie zabezpieczonego dysku jest niemożliwe. W praktyce oznacza to utratę całego dysku wraz z zawartymi na nim danymi, co może być problemem dla wielu użytkowników. Jednak dla użytkowników wspomnianych na początku tej części (tzn. ceniących sobie bezpieczeństwo danych) ryzyko utraty dysku i danych bez możliwości ich odczytania przez osoby nieupoważnione jest do przyjęcia.

Korzystanie z funkcji DriveLock

Opcja DriveLock jest dostępna w menu Security (Zabezpieczenia) programu Computer Setup. W tym menu możliwe jest ustawienie hasła głównego lub włączenie funkcji DriveLock. Jeżeli funkcja DriveLock ma zostać włączona, należy podać hasło użytkownika. Ponieważ funkcja ta jest zwykle najpierw konfigurowana przez administratora systemu, jako pierwsze musi zostać ustawione hasło główne. Ustawienie tego hasła jest zalecane, jeżeli planowane jest włączenie funkcji DriveLock, jak również jeżeli funkcja ta nie ma być używana. Umożliwi to administratorowi zmianę ustawień tej opcji w przypadku zablokowania dysku w przyszłości. Po ustawieniu hasła administrator systemu może włączyć funkcję DriveLock lub pozostawić ją wyłączoną.

Jeżeli w systemie zostanie wykryty zablokowany dysk twardy, podczas autotestu POST konieczne będzie podanie odpowiedniego hasła. Jeżeli ustawione jest hasło uruchomieniowe i jest ono takie samo, jak hasło użytkownika urządzenia, podczas autotestu POST nie pojawi się monit o wprowadzenie hasła. W przeciwnym wypadku użytkownik otrzyma monit o podanie hasła funkcji DriveLock. Można wprowadzić również hasło główne. Użytkownik może podjąć dwie próby wprowadzenia poprawnego hasła. Jeżeli odpowiednie hasło nie zostanie wprowadzone, autotest POST będzie kontynuowany, ale zablokowany dysk będzie niedostępny.

Zastosowania funkcji DriveLock

Najbardziej praktycznym zastosowaniem funkcji zabezpieczeń DriveLock jest korzystanie z niej w środowisku korporacyjnym, w którym administrator systemu udostępnia użytkownikom niektórych komputerów dyski twarde MultiBay. Administrator systemu jest odpowiedzialny za skonfigurowanie dysku twardego MultiBay, co jest między innymi związane z ustawieniem hasła głównego funkcji DriveLock. W przypadku utraty hasła użytkownika lub przekazania komputera innemu pracownikowi zmiana hasła użytkownika i uzyskanie ponownego dostępu do dysku są możliwe za pomocą hasła głównego.

Zalecane jest, aby administratorzy systemu w przedsiębiorstwach, w których stosowana jest funkcja DriveLock, ustanowili ogólne zasady dotyczące ustawiania i obsługi haseł głównych. Jeżeli zasady te nie zostaną ustanowione, może wystąpić sytuacja, w której oba hasła funkcji zostaną ustawione (celowo bądź przez przypadek) przez pracownika na krótko przed zakończeniem jego zatrudnienia (np. z powodu zwolnienia lub przejścia na emeryturę). Po odejściu pracownika zablokowany przez niego dysk nie będzie mógł być używany i konieczna będzie jego wymiana. Podobnie jeżeli administrator nie ustawi hasła głównego, może nie być możliwe przeprowadzenie sprawdzenia zainstalowanego oprogramowania oraz obsługa innych funkcji kontroli dostępu.

Włączanie funkcji DriveLock nie jest zalecane w przypadku użytkowników, których wymagania dotyczące bezpieczeństwa danych nie są tak wysokie. Kategoria ta obejmuje użytkowników indywidualnych oraz użytkowników, którzy nie przechowują zwykle na swoich dyskach poufnych danych. Dla tych użytkowników ostateczne zablokowanie dysku spowodowane utratą obu haseł funkcji DriveLock jest znacznie bardziej kosztowne niż ewentualne udostępnienie zapisanych na nim danych. Dostęp do opcji DriveLock (i programu Computer Setup) może zostać ograniczony przy użyciu hasła konfiguracyjnego. Przez określenie hasła konfiguracyjnego i zablokowanie dostępu do niego przez użytkowników końcowych, administratorzy systemów mogą ograniczyć użytkownikom możliwość włączania funkcji DriveLock.

Czujnik Smart Cover Sensor

Smart Cover Sensor to dostępna w wybranych modelach komputera funkcja będąca połączeniem technologii sprzętowych i programowych, która może wysyłać alerty informujące o zdjęciu obudowy lub panelu dostępu komputera. Czujnik ten oferuje trzy poziomy zabezpieczeń, opisane w poniższej tabeli.

Poziomy zabezpieczeń czujnika Smart Cover Sensor

Poziom	Ustawienie	Opis
Poziom 0	Wyłączony	Czujnik Smart Cover Sensor jest wyłączony (ustawienie domyślne)
Poziom 1	Powiadamianie użytkownika	Po ponownym uruchomieniu komputera na ekranie pojawi się komunikat informujący o zdjęciu obudowy lub panelu bocznego komputera.
Poziom 2	Hasło konfiguracyjne	Po ponownym uruchomieniu komputera na ekranie pojawi się komunikat informujący o zdjęciu obudowy lub panelu bocznego komputera. Aby kontynuować, należy wprowadzić hasło konfiguracyjne.

Ustawienia te można zmieniać w programie Computer Setup. Więcej informacji o programie Computer Setup znajduje się w *Podręczniku do programu Computer Setup (F10)*.

Ustawianie poziomów zabezpieczeń czujnika Smart Cover Sensor

Aby ustawić poziom zabezpieczeń czujnika Smart Cover Sensor, wykonaj poniższe czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

3. Wybierz menu **Security (Zabezpieczenia)**, wybierz opcję **Smart Cover (Czujnik Smart Cover)**, a następnie postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

Blokada Smart Cover Lock

Smart Cover Lock jest sterowaną programowo blokadą obudowy komputera dostępną w wybranych komputerach firmy HP. Blokada zapobiega nieautoryzowanemu dostępowi do wewnętrznych elementów komputera. Komputer jest dostarczany z wyłączoną blokadą Smart Cover Lock.

PRZESTROGA: Aby zabezpieczyć ustawienia blokady Smart Cover Lock, należy pamiętać o ustawieniu hasła konfiguracyjnego. Hasło to zapobiega nieautoryzowanemu dostępowi do programu Computer Setup.

Blokada Smart Cover Lock jest dostępna jako opcja w niektórych systemach.

Włączanie blokady Smart Cover Lock

Aby włączyć blokadę Smart Cover Lock, wykonaj poniższe czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

3. Wybierz menu **Security (Zabezpieczenia)**, wybierz opcję **Smart Cover (Blokada Smart Cover)**, a następnie ustaw opcję **Locked (Włączona)**.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

Wyłączanie blokady Smart Cover Lock

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

3. Wybierz kolejno **Security (Zabezpieczenia) > Smart Cover > Unlocked (Wyłączona)**.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

Używanie klucza Smart Cover FailSafe Key

Jeżeli włączona jest blokada Smart Cover Lock i z różnych powodów nie można wprowadzić wyłączającego ją hasła konfiguracyjnego, obudowę komputera można otworzyć za pomocą klucza Smart Cover FailSafe Key. Sytuacje, w których niezbędne jest użycie klucza to:

- brak zasilania,
- błąd podczas uruchamiania komputera,
- wadliwe elementy komputera (np. wadliwy procesor lub zasilacz),
- utrata hasła.

PRZESTROGA: Klucz Smart Cover FailSafe Key jest specjalistycznym narzędziem dostępnym w firmie HP. Ze względu na duże prawdopodobieństwo wystąpienia wymienionych wyżej sytuacji, klucz taki najlepiej zamówić odpowiednio wcześniej u autoryzowanego sprzedawcy lub serwisanta produktów firmy Compaq.

Aby nabyć klucz FailSafe Key, należy:

- Skontaktować się z autoryzowanym sprzedawcą lub serwisantem produktów firmy HP.
- Zadzwonić pod odpowiedni numer wskazany w gwarancji.

Więcej informacji dotyczących korzystania z klucza Smart Cover FailSafe Key można znaleźć w *Instrukcji obsługi sprzętu*.

Zabezpieczenie głównego rekordu rozruchowego

Główny rekord rozruchowy (Master Boot Record, MBR) zawiera informacje wymagane do pomyślnego uruchomienia systemu z dysku i uzyskania dostępu do danych przechowywanych na tym dysku. Funkcja zabezpieczenia głównego rekordu rozruchowego umożliwia cofnięcie wprowadzonych przypadkowo lub omyłkowo zmian tego rekordu (np. spowodowanych działaniem wirusów lub niewłaściwym wykorzystaniem narzędziowych programów dyskowych). Możliwe jest również odtworzenie tej wersji rekordu, przy której nastąpiło ostatnie poprawne uruchomienie systemu.

Aby włączyć zabezpieczenie głównego rekordu rozruchowego, wykonaj następujące czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

---

3. Wybierz kolejno **Security (Zabezpieczenia) > Master Boot Record Security (Zabezpieczenie głównego rekordu rozruchowego) > Enabled (Włączone)**.
4. Wybierz kolejno **Security (Zabezpieczenia) > Save Master Boot Record (Zapisz główny rekord rozruchowy)**.
5. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

Po włączeniu zabezpieczenia głównego rekordu rozruchowego system BIOS uniemożliwia wprowadzenie zmian w tym rekordzie na bieżącym dysku rozruchowym w trybie MS-DOS lub w trybie awaryjnym systemu Windows.

Większość systemów operacyjnych umożliwia dostęp do głównego rekordu rozruchowego na bieżącym dysku rozruchowym. W przypadku korzystania z jednego z takich systemów BIOS nie jest w stanie przeciwdziałać wprowadzaniu zmian w tym rekordzie.

Przy każdym włączaniu lub ponownym uruchamianiu komputera główny rekord rozruchowy dysku rozruchowego jest porównywany z poprzednio zapisanymi ustawieniami MBR. Jeżeli wykryte zostaną zmiany, a poprzednio zapisany główny rekord rozruchowy należał do bieżącego dysku rozruchowego, wyświetlany jest następujący komunikat:

1999—Master Boot Record has changed.

Press any key to enter Setup to configure MBR Security.

Po uruchomieniu programu Computer Setup należy:

- zapisać główny rekord rozruchowy bieżącego dysku startowego,
- odtworzyć zapisany poprzednio główny rekord rozruchowy LUB
- wyłączyć zabezpieczenie rekordu MBR.

Do wykonania tych czynności niezbędne jest wprowadzenie hasła konfiguracyjnego (jeżeli zostało ono ustawione).

Jeżeli wykryte zostaną zmiany, a poprzednio zapisany główny rekord rozruchowy **nie** należał do bieżącego dysku rozruchowego, wyświetlany jest następujący komunikat:

2000—Master Boot Record Hard Drive has changed.

Press any key to enter Setup to configure MBR Security.

Po uruchomieniu programu Computer Setup należy:

- zapisać główny rekord rozruchowy bieżącego dysku startowego LUB
- wyłączyć zabezpieczenie rekordu MBR.

Do wykonania tych czynności niezbędne jest wprowadzenie hasła konfiguracyjnego (jeżeli zostało ono ustawione).

Jeżeli poprzednio zapisany główny rekord rozruchowy został uszkodzony (chociaż zdarza się to bardzo rzadko), wyświetlany jest następujący komunikat:

1998—Master Boot Record has been lost.

Press any key to enter Setup to configure MBR Security.

Po uruchomieniu programu Computer Setup należy:

- zapisać główny rekord rozruchowy bieżącego dysku startowego LUB
- wyłączyć zabezpieczenie rekordu MBR.

Do wykonania tych czynności niezbędne jest wprowadzenie hasła konfiguracyjnego (jeżeli zostało ono ustawione).

Czynności wykonywane przed partycjonowaniem lub formatowaniem bieżącego dysku rozruchowego

Przed partycjonowaniem lub formatowaniem bieżącego dysku rozruchowego należy wyłączyć funkcję zabezpieczenia rekordu MBR. Główny rekord rozruchowy może być aktualizowany przez niektóre dyskowe programy narzędziowe (np. FDISK lub FORMAT). Jeżeli zabezpieczenie rekordu MBR pozostanie włączone, podczas partycjonowania lub formatowania dysku mogą pojawić się komunikaty o błędach wykrytych przez wymienione programy narzędziowe, a po ponownym uruchomieniu komputera może także zostać wyświetlone ostrzeżenie związane z zabezpieczeniem.
Aby wyłączyć zabezpieczenie głównego rekordu rozruchowego, wykonaj następujące czynności:

1. Włącz lub uruchom ponownie komputer. W systemie Windows kliknij kolejno **Start > Zamknij > Uruchom ponownie komputer**.
2. Kiedy znajdująca się na monitorze dioda zaświeci się na zielono, naciśnij klawisz **F10**. W razie potrzeby możesz nacisnąć klawisz **Enter**, aby pominąć ekran tytułowy.

Jeśli klawisz **F10** nie zostanie naciśnięty w odpowiednim czasie, dostęp do programu będzie możliwy dopiero po wyłączeniu, a następnie ponownym uruchomieniu komputera i naciśnięciu klawisza **F10**.

3. Wybierz kolejno **Security (Zabezpieczenia) > Master Boot Record Security (Zabezpieczenie głównego rekordu rozruchowego) > Disabled (Wyłączone)**.
4. Przed wyjściem z programu kliknij kolejno **File (Plik) > Save Changes and Exit (Zapisz zmiany i zakończ)**.

Zabezpieczająca blokada kablowa

Z tyłu komputera znajduje się gniazdo blokady kablowej, umożliwiające przymocowanie komputera do nieruchomego obiektu przy stanowisku pracy.

Szczegółowe instrukcje (wraz z rysunkami) można znaleźć w *Instrukcji obsługi sprzętu* na dysku CD *Biblioteka z dokumentacją*.

Identyfikacja na podstawie analizy linii papilarnych

Dzięki wprowadzeniu opracowanej przez firmę HP technologii identyfikacji użytkownika na podstawie analizy linii papilarnych przestaje być konieczne wprowadzanie haseł, a tym samym podnosi się poziom bezpieczeństwa w sieci, uproszczeniu ulega proces logowania, a także obniżają się koszty związane z zarządzaniem siecią komputerową przedsiębiorstwa. Rozwiązanie to stało się dostępne po atrakcyjnej cenie dla wielu przedsiębiorstw, nie tylko tych wysoko zaawansowanych technologicznie i korzystających z rozbudowanych systemów zabezpieczeń.

W zależności od modelu technologia ta jest wykorzystywana w różny sposób.

Więcej informacji można znaleźć na stronie:

http://h18000.www1.hp.com/solutions/security.

Powiadamianie o usterkach i ich usuwanie

Funkcja powiadamiania o usterkach i ich usuwania łączy w sobie zalety nowoczesnej technologii sprzętowej i programowej, dzięki czemu znacznie obniża ryzyko utraty istotnych danych oraz wystąpienia nieplanowanych przestojów w pracy.

W przypadku wystąpienia usterki wyświetlany jest komunikat alertu lokalnego, zawierający jej opis i zalecane czynności do wykonania. Przy użyciu programu HP Client Manager można również zapoznać się z informacjami na temat bieżącego stanu systemu. Jeśli komputer jest podłączony do sieci pracującej pod kontrolą programu HP Insight Manager, HP Client Manager lub innych aplikacji do zarządzania systemem, powiadomienie o usterce jest również przesyłane do tej aplikacji.

System ochrony dysków

System ochrony dysków Drive Protection System (DPS) jest narzędziem diagnostycznym, zintegrowanym z dyskami twardymi instalowanymi w wybranych typach komputerów osobistych HP. System ten ułatwia diagnozowanie problemów, w wyniku których mogłaby zaistnieć potrzeba nieobjętej gwarancją wymiany dysku twardego.

Podczas montażu komputerów firmy HP każdy instalowany w nich dysk twardy jest testowany przy użyciu programu DPS, a kluczowe informacje są na nim zapisywane na stałe. Każdorazowe uruchomienie programu DPS powoduje zapisanie wygenerowanych przez niego wyników na dysku twardym. Informacje te mogą pomóc serwisantowi w zdiagnozowaniu warunków, które spowodowały uruchomienie oprogramowania DPS. Informacje dotyczące używania systemu DPS znajdują się w *Podręczniku rozwiązywania problemów.*

Zasilacz z zabezpieczeniem antyprzepięciowym

Zintegrowany zasilacz z zabezpieczeniem antyprzepięciowym zapewnia większą niezawodność pracy komputera w przypadku wystąpienia gwałtownych zmian napięcia w sieci. Bez ryzyka utraty danych i przestojów systemu wytrzymuje on skoki napięcia do 2000 V.

Czujnik termiczny

Czujnik termiczny, łącząc w sobie funkcje programowe i sprzętowe, jest urządzeniem rejestrującym temperaturę wewnątrz komputera. W momencie przekroczenia dopuszczalnej temperatury wyświetlany jest odpowiedni komunikat. Dzięki odpowiednio wczesnemu ostrzeżeniu użytkownik może podjąć odpowiednie kroki, które zapobiegną uszkodzeniu komputera i utracie danych.

Indeks

I

K

N

O

P

R

S

Ś

T

U

W

Z